

## Operationalizing Risk Management per ICD-503

### Securing Government IP-Based Information Technology Infrastructure – including Industrial Control Systems and Critical Infrastructure – via Proactive Service Assurance

In the rush to exploit the advances in information technology, including procurement mandates driving adoption of commercial-off-the-shelf (COTS) technology, additional layers of complexity can bury, create or expose weaknesses in the software within these increasingly IP-based net-centric systems. The shared risk of a poorly designed product or system being deployed often has far-reaching impacts across the network. Both corporate and government organizations employ security certification processes to ensure that these new network capabilities do not introduce unplanned security vulnerabilities or risk into the organizational community of interest.

In order to assist the implementation of these processes, various regulatory bodies (or government agencies) have defined management guidelines applicable to IT functions, including procurement. To date, it has been difficult to expedite and automate the process flow of Information Assurance with useful security and/or service availability metrics throughout the IA life cycle (e.g., providing for automation and regression testing).

Mu Dynamics has developed the process-adaptable Mu Service Analyzer that endows the entire IA life cycle with actionable reliability, availability and security metrics. Figure 1 shows the IA life cycle on the left, and the parallel vendor or developer life cycle on the right. The two cycles are related, and change management and project management processes benefit from the significant opportunity for feedback between the two. Besides the actual mechanics of testing services by generating either millions of variations on service traffic, or simulating denial of service conditions, or replaying traffic designed to trigger known vulnerabilities, the Mu analyzer is an integral part of a complete automated test harness.

The Mu analyzer appliance can be integrated into test environments based on web-2.0 technology (exposed via Web Services Description Language, WSDL), or via its web-based REST interface, or by its direct support for HP Quality Center. In other situations, e.g., smaller environments, the Mu analyzer is powerful enough on its own to be the test

conductor and repository of past data, integrating with any device control-able via an SSH or Telnet interface and reaching out to monitor the network using many dozens of protocols.

Regarding the two parallel life cycles in the information assurance world, the Mu analyzer facilitates the certification and accreditation flow by providing detailed fault records (including remediation tools such as packet captures, and executable “live exploits”) to enable productive collaboration between network operators, government organizations or industrial control systems operators and their respective equipment vendors by communicating actionable fault details to their vendors to minimize the mean-time-to-repair (MTTR) for any issue.

### NIST Study Shows >10x Savings Through Proactive Software Testing

NIST has studied the product development and deployment processes and documented a substantial ROI multiplier for early adoption of methodologies that reduces the number of service weaknesses (for end-users) and bugs (for vendors).

NIST's report is available at this URL:

<http://www.nist.gov/director/prog-ofc/report02-3.pdf>.

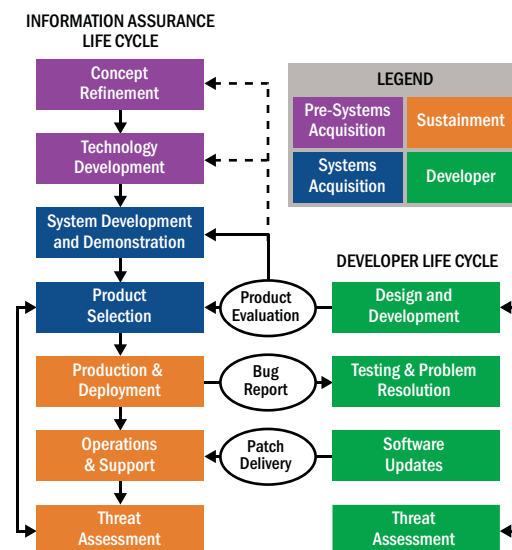


Figure 1: Information Assurance Life Cycle

The benefit of applying the Mu analyzer for both end-users and vendors is similar: Reduction in overhead due to field fire drills and the significant reduction in life cycle cost that accrues from shifting the discovery of software bugs to as early as possible in the product development or deployment life cycle. The most significant benefit for the government information assurance practice derives from driving the risk management and risk reduction mentality as close as possible to the beginning of the information assurance life cycle: as early as the requirements definition and vendor selection processes. The best way to reduce risk while also keeping life cycle costs down is to ensure that the most

reliable, available and secure devices are purchased. Then, when products are placed into service, they are continuously evaluated based on the initial configuration and this baseline is referenced proactively throughout the remainder of the product's or service's lifetime.

*There is an unquestionable ROI benefit of applying thorough testing and evaluation procedures from the earliest stages of the service deployment or product development life cycles.*

### **Mapping to Intelligence Community Directive (ICD) number 503 (ICD-503)**

The central theme of ICD-503 is the certification and accreditation of computer networking (Information Technology) assets in the context of usage by the Intelligence Community (IC). The goal is to reduce risk to these systems by improving reliability and availability, and especially security. There is an unquestionable ROI benefit of applying thorough testing and evaluation procedures from the earliest stages of the service deployment or product development life cycles. However, the real win comes from applying "continuous improvement" throughout the entire life cycle, across patch management, change management, etc. so that the effort invested at the beginning of the process isn't limited to a single point in time. ICD-503 in fact states up front that the focus is on a "more holistic and strategic process for the risk management of information technology systems, and on processes and procedures designed to develop trust across the intelligence community information technology enterprise through the use of common standards and reciprocally accepted certification

and accreditation decisions." The Mu service analyzer automates ICD-503 testing for government agencies, either intelligence community or otherwise, through an ongoing closed-loop compliance process that spans across any information assurance certification and accreditation procurement or operational activity.

### **Applicability to Industrial Control Systems and Critical Infrastructure Applications of Information Technology**

As the migration to IP-based systems grows, it even permeates areas such as industrial control systems that formerly used proprietary networking technologies. Besides being proprietary, these systems were also not connected to the outside world. The transition to IP-based networking brings risks, both from the introduction of unfamiliar software stacks used in new types of deployments, and from opportunities for interconnection of formerly isolated networks with non-industrial control system networks. The U.S. Government Accountability Office (GAO) has described a dramatic new escalation in security risks to industrial control systems, citing four areas of concern:

1. adoption of standardized technologies with known vulnerabilities
2. control networks being connected to other networks
3. having insecure connections, which exacerbate vulnerabilities
4. having information about infrastructures and control systems be easily available to the public

These specific GAO observations and recommendations are online: <http://www.gao.gov/cgi-bin/getrpt?GAO-04-354>.

Given that ICD-503 and other Information Assurance processes center on managing life cycle costs as well as program risk, GAO observations are concerning and raise the importance of the risk management processes embodied in ICD-503. Ignoring or improperly addressing industrial control system

*In addition to physical safety and security, network security for critical infrastructure is crucial for risk mitigation because of reliance on electronic systems for operational control.*



*IA/Security is more leadership, strategic direction, than technical!" – Mike Davis, US Navy*

security or robustness risks creates the opportunity for disruption of critical systems, damage to equipment, and may cause unpredictable operations or failure of critical infrastructure. The US Government has enumerated a list of vital critical infrastructure sectors, including IT assets supporting agriculture, food, water, public health, emergency services, defense industrial base, telecommunications, energy, transportation, banking and finance, chemical, postal and shipping, and key physical assets such as nuclear power plants, dams, government facilities and commercial assets.

In addition to physical safety and security, network security for critical infrastructure is crucial for risk mitigation because of reliance on electronic systems for operational control. Malfunctions to the industrial control systems in these industries, including faults within networked assets including programmable logic controllers (PLCs), intelligent electronic devices (IEDs) and remote terminal units (RTUs) are proactively identified and safely removed through a Mu-enabled testing process. Lacking a well-defined safety and security test regime causes safety issues resulting in physical injury or death, business or social disruption, weakened national

security, environmental damage, and damage to the reputation of the business or agency, possibly stimulating a desire for increased regulation or oversight. Similar to other IP-based technology domains (i.e., VoIP, IMS, IPTV, data services), there is an opportunity for a new level of collaboration between operators and vendors within the industrial control systems ecosystem -- whether or not the application is deemed "critical infrastructure."

#### **Conclusion**

In all cases, the goal is to quickly achieve program goals while containing costs and reducing safety and security risks across the entire product development or service deployment life cycle. It is possible to proactively embed actionable testing for reliability, availability and security into these programs in a way that adds little overhead while reducing risk across the product or service life cycle. These best practices also reduce overall system and program costs, as well as costly unplanned overhead due to fire drills where staff are forced to deal with emergencies due to previously hidden software weaknesses.

The Mu Service Analyzer offers operators of industrial control systems – and the developers of the products on which they depend – a customizable system for maximizing operational safety and efficiency over IP networks. The Mu analyzer helps improve uptime, reduces time spent on product safety workarounds or costly security breaches by averting successful exploits of IP-related vulnerabilities, and limits problems caused by insufficiently robust implementations of the underlying network protocols. The Mu analyzer helps both operators and their product vendors suppliers with the

identification and timely repair of reliability, availability and security issues and provides customizable metrics that enable management oversight across the entire life cycle. Cost-effective and dynamic comprehensive test suites allow the Mu analyzer to address all major protocols affecting government information technology assets, including critical infrastructure, providing an essential and easy-to-deploy way to benchmark system safety and enable security within a process of continuous improvement.

### Top Ten Steps Representing an Overall IA/Security Approach

1. Comprehensive security policy (goes hand-in-hand with communication and enforcement!)
2. Distribute clear governance (who does what and when, R&R, resources, ROE)
3. Build defense-in-depth (maintain multiple fronts)
4. Follow a strategy, master plan (use an enterprise architecture)
5. Configuration management (automated reporting to enable enforcement)
6. Develop an effective tool suite (stress automation and keep-it-simple (KISS))
7. Guard major threat entry points (phased attacks, root kits, phishing)
8. Guard malware entry methods (monitor web, filter content filter and block URLs)
9. Test critical elements (COOPs, training, compliance, vulnerabilities)
10. Risk management plan (current threats, vulnerabilities and impacts)

### Quick-Reference-Guide to U.S. Government IA/Security Resources

#### Primary Sites

- \* <https://infosec.navy.mil/docs/index.jsp>
- \* <https://www.fleetforces.navy.mil/netwarcom/navycanda>
- \* <http://isae.disa.mil/ditscap/>

#### Other Useful IA/Security Sites

- \* <https://www.us.army.mil/suite/portal/index.jsp>
- \* <http://csrc.nist.gov>
- \* <http://www.nsa.gov/ia/index.cfm>
- \* <http://www.iatf.net/>
- \* <http://www.cert.org/>
- \* <http://www.sse-smm.org/lib/lib.asp>
- \* <http://www.commoncriteriaportal.org/>
- \* [http://www.amc.army.mil/amc/ci/matrix/policy/policy\\_new.htm](http://www.amc.army.mil/amc/ci/matrix/policy/policy_new.htm)
- \* <https://www.sans.org/about/sans.php>
- \* <http://iac.dtic.mil/iatac>
- \* <http://www.cerias.purdue.edu>
- \* <http://security.sdsc.edu/>
- \* <http://iase.disa.mil/stigs/index.html>



web: [www.mudynamics.com](http://www.mudynamics.com) | email: [info@mudynamics.com](mailto:info@mudynamics.com)  
address: 686 W. Maude Ave., Suite 104, Sunnyvale, CA 94085, USA  
phone: (866) 276-4640 or (408) 329-6330 | fax: (408) 329-6317